

Partial Translation of Citation 2 (JP No. 11-25045)

Referring to Fig. 8, an operation of an apparatus for issuing an attribution certification will be explained below.

At first, an ID and attribute of an access object (or user) are transferred to a text making apparatus 21 where a text of an attribute certification is created. The certification is stored in a text storage apparatus 602. Next, a signature making apparatus 22 reads a private key of an attribution CA from a private key storage apparatus 601, and using the private key, executes a digital signature to the text of the attribute certificate stored in the text storage apparatus 602 to create a signed (or encrypted) text. The resultant signed text is stored in a signed text storage apparatus 603. Finally, a certificate creation apparatus 23 creates an attribute certificate from the text stored in the text storage apparatus 602 and the signed text stored in the signed text storage apparatus 603.

特開平11-25045

(43)公開日 平成11年(1999)1月29日

(51)Int.Cl. ⁶		識別記号		F I	
G 0 6 F	15/00	3 3 0		G 0 6 F	15/00 3 3 0 A
	12/14	3 1 0			12/14 3 1 0 K
H 0 4 L	9/32			H 0 4 L	9/00 6 7 5 B

審査請求 有 請求項の数27 FD (全 23 頁)

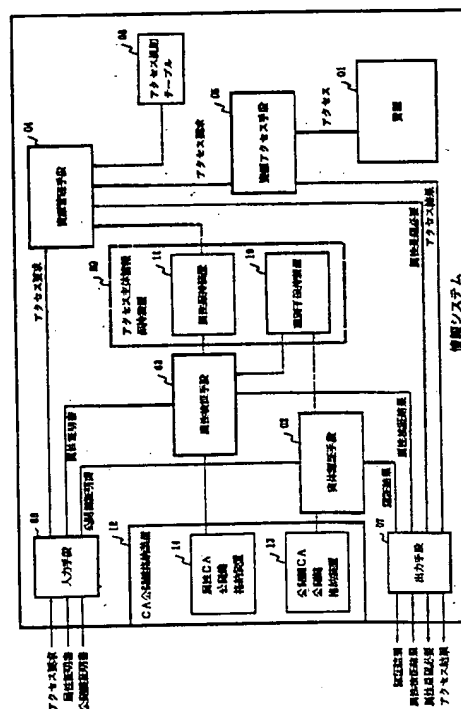
(21)出願番号	特願平9-189041	(71)出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22)出願日	平成9年(1997)6月30日	(72)発明者	山岡 善侍 東京都港区芝五丁目7番1号 日本電気株 式会社内
		(74)代理人	弁理士 境 廣巳

(54)【発明の名称】 アクセス制御方法とその装置及び属性証明書発行装置並びに機械読み取り可能な記録媒体

(57) 【要約】

【課題】 アクセス主体を知らなくてもアクセス規則の設定を単純に行うことができ、しかも、アクセス主体が権限を持つことの確認も可能で、さらに、ユーザ管理の容易なアクセス制御の方法を提供する。

【解決手段】 アクセス主体の一部の情報を与える、或いはアクセス主体の特性を記述するデータを、属性と定義する。アクセス規則テーブル08は、情報システム内に全ての資源01毎にそのアクセスに必要な属性を設定してある。実体認証手段02でアクセス主体の実体認証を行い、属性検証手段03でアクセス主体の属性の認否の判定を行い、資源管理手段04で資源01に対するアクセス主体からのアクセス要求の可否を判定する。属性の認否の判定には、アクセス主体が提示する属性証明書を用いる。



【特許請求の範囲】

【請求項1】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する方法において、アクセス主体の属性によりアクセス規則を設定し、アクセス主体の属性を是認することで制御を行うことを特徴とするアクセス制御方法。

【請求項2】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する方法において、アクセス主体の属性によりアクセス規則を設定し、アクセス主体の実体認証を行い、アクセス主体の属性を是認することで制御を行うことを特徴とするアクセス制御方法。

【請求項3】 アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により、アクセス規則を設定することを特徴とする請求項1または2記載のアクセス制御方法。

【請求項4】 アクセス主体の属性の是認を属性情報テーブルを用いることにより行うことを特徴とする請求項1、2または3記載のアクセス制御方法。

【請求項5】 アクセス主体の属性の是認をアクセス主体が提示してきた属性情報に対して行うことを特徴とする請求項1、2または3記載のアクセス制御方法。

【請求項6】 アクセス主体の属性の提示をデジタル署名を施された属性証明書を用いることにより行うことを特徴とする請求項5記載のアクセス制御方法。

【請求項7】 アクセス主体の属性の提示を公開鍵証明書を用いることにより行うことを特徴とする請求項5記載のアクセス制御方法。

【請求項8】 アクセス主体の実体認証をパスワードにより行うことを特徴とする請求項2、3、4、5または6記載のアクセス制御方法。

【請求項9】 アクセス主体の実体認証を公開鍵証明書を用いることにより行うことを特徴とする請求項2、3、4、5、6または7記載のアクセス制御方法。

【請求項10】 アクセス主体の実体認証をデジタル署名を施された属性証明書を用いることにより行うことを特徴とする請求項2、3、5または6記載のアクセス制御方法。

【請求項11】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装置において、アクセス主体の属性によりアクセス規則を設定するテーブルを備えることを特徴とするアクセス制御装置。

【請求項12】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装置において、アクセス主体の属性によりアクセス規則を設定するテーブルと、アクセス主体の属性を是認する手段とを備えることを特徴とするアクセス制御装置。

【請求項13】 情報システムの資源に対するアクセス主体からのアクセスをアクセス規則に基づき制御する装

置において、アクセス主体の属性によりアクセス規則を設定するテーブルと、アクセス主体の属性を是認する手段と、アクセス主体の実体認証を行う手段とを備えることを特徴とするアクセス制御装置。

【請求項14】 アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により、アクセス規則を設定するテーブルを備えることを特徴とする請求項11、12または13記載のアクセス制御装置。

【請求項15】 属性情報を保存したテーブルを参照し属性を是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項16】 属性情報を記載した属性証明書を検証して属性を是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項17】 属性情報を記載した公開鍵証明書で認証して属性を是認する手段を備えることを特徴とする請求項12、13または14記載のアクセス制御装置。

【請求項18】 パスワードにより実体認証する手段を備えることを特徴とする請求項13、14、15または16記載のアクセス制御装置。

【請求項19】 公開鍵証明書を用いることにより実体認証する手段を備えることを特徴とする請求項13、14、15、16または17記載のアクセス制御装置。

【請求項20】 属性証明書を用いることにより実体認証する手段を備えることを特徴とする請求項13、14または16記載のアクセス制御装置。

【請求項21】 アクセス主体の属性から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項22】 アクセス主体の属性と識別子から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項23】 アクセス主体の属性と公開鍵から属性証明書本文を作成する手段と、属性証明書本文にデジタル署名を行い属性証明書署名文を作成する手段と、属性証明書本文と属性証明書署名文から属性証明書を作成する手段とを備えることを特徴とする属性証明書発行装置。

【請求項24】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、パスワード照合によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の

成功後に、アクセス主体が資源にアクセスするために必要な属性を保有しているか否かを、各アクセス主体の属性を設定してある属性情報テーブルおよび前記アクセス規則を設定してあるアクセス規則テーブルを参照して判断するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項25】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する公開鍵証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、アクセス主体が資源にアクセスするために必要な属性を保有しているか否かを、各アクセス主体の属性を設定してある属性情報テーブルおよび前記アクセス規則を設定してあるアクセス規則テーブルを参照して判断するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項26】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する公開鍵証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、アクセス主体が提示する属性証明書によりアクセス主体の属性を是認するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限するステップと、是認したアクセス主体の属性と前記アクセス規則を設定してあるアクセス規則テーブルとに基づいて資源に対するアクセス主体からのアクセスの可否を判断するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【請求項27】 情報システムの資源に対するアクセス主体からのアクセスを、アクセス主体の属性により記述されたアクセス規則に基づき制御するプログラムであって、コンピュータに、アクセス主体が提示する、アクセス主体の公開鍵及び属性を証明する証明書によりアクセス主体の実体認証を行うステップと、アクセス主体の実体認証が成功するまでアクセス主体からの資源に対するアクセスを制限するステップと、アクセス主体の実体認証の成功後に、前記証明書によりアクセス主体の属性を是認するステップと、アクセス主体の属性が是認されるまでアクセス主体からの資源に対するアクセスを制限す

るステップと、是認したアクセス主体の属性と前記アクセス規則を設定してあるアクセス規則テーブルとに基づいて資源に対するアクセス主体からのアクセスの可否を判断するステップとを行わせるプログラムを記録した機械読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報システム内の資源に対するユーザなどのアクセスを制御する方法および装置に関する。

【0002】

【従来の技術】従来、情報システムのアクセス制御は、資格のないアクセス主体の接近から、内部の資源を守るために、アクセス規則を設定して、その規則に応じて、資源へのアクセスを制限することにより、資源の保護を行ってきた。ここで、アクセス主体とは、ユーザ、プロセス、機器、などのことを表し、また、資源とは、データ、ファイル、プログラム、アプリケーション、サービス、機器、などのことを表す。「暗号とデータセキュリティ」(D.E.R.デニング著、1988年発行、培風館)の4章や、「情報システムのセキュリティ」(上園忠広著、1995年発行、トッパン)のP.143～155には、アクセス制御について、詳しく述べられている。

【0003】アクセス規則の設定には、アクセス権限行列、あるいは、許可リスト、資格リストなどのテーブルが用いられる。アクセス権限行列とは、アクセス主体の資源に対する権限が定義された行列である。権限とは、読み出し可能、書き込み可能、更新可能、削除可能、実行可能、などの機能のことである。許可リストは、特定の資源に対して設定されたリストであり、アクセス主体の権限を定義する。資格リストは、特定のアクセス主体に対して設定されたリストであり、資源に対する権限を定義する。

【0004】情報システムでアクセス規則を設定するためには、情報システムでアクセス主体を識別することが必要になり、各アクセス主体に対して識別子を用意することで、その識別子を用いてアクセス規則の設定を行っている。

【0005】アクセス規則の設定を簡易に行うための方法としては、アクセス主体を何らかの基準に応じてグループ化して、そのグループに対してアクセス規則を設定する方法がある。

【0006】しかし、例えば、アクセス主体がユーザのとき、識別子を用意するだけでは、ユーザが本当に本人であるということを保証できない。そのため、ユーザが正当であることを確認する実体認証の技術も重要になる。実体認証の方法としては、パスワードの入力がよく用いられている。この方法では、識別子・パスワードの対になったパスワード情報を参照することにより、実体認証を行う。

【0007】ユーザに識別子を用意すること、および、パスワード情報を設定することは、一般にユーザ登録と呼ばれている。

【0008】結局、従来の情報システムでアクセス制御を行うためには、ユーザ登録により、ユーザ識別、ユーザ認証を行うことが前提になる。

【0009】また、実体認証の方法としては、非対称暗号系を用いる方法がある。非対称暗号系とは、一般に公開された公開鍵と本人のみが秘密に持つ秘密鍵により、暗号化・復号を行う技術である。実体認証に用いる場合は、秘密鍵の所持により本人であることを主張する。非対称暗号系を実体認証に用いる方法については、米国特許の4,405,829,「CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD」や、ISO/IEC9793-3「Information technology-Security techniques-Entity authentication mechanisms-Part3: Entity authentication using a public key algorithm」に詳しく述べられている。

【0010】デジタル署名は、文書の作成者が本人であること、文書の正当性・完全性、を確認する技術であり、主に非対称暗号系を利用する。この場合、秘密鍵で署名文の作成を行い、公開鍵で署名の確認を行う。「E-Mailセキュリティ」(Bruce Schneier 著、1995年、オーム社)の第4章では、デジタル署名について詳しく述べられている。

【0011】非対称暗号系では、公開鍵が偽造されたものでないことの証明のために、信頼できる第三者によるデジタル署名をつけた公開鍵証明書を発行する。証明書を発行する機関はCAと呼ばれる。上記「E-Mailセキュリティ」の第5章では、公開鍵証明書、CAについて詳しく述べられている。ここでは、特にCAを公開鍵CAと呼ぶことにする。

【0012】

【発明が解決しようとする課題】従来の技術では、情報システムで、ある資格を持ったユーザに何らかのサービスを提供する場合、ユーザ単位にアクセス規則を設定し、アクセスを制御する。しかし、この方法では、第1の問題として、ユーザを識別、実体認証できなければならないので、情報システムごとに事前のユーザ登録が必要になる点が挙げられる。また、第2の問題として、アクセス規則の設定は、登録ユーザごとに行わなくてはならない点が挙げられる。さらに、第3の問題として、アクセス主体自身とアクセス主体が権限を持つ資格があるかどうかを知っていなければ、アクセス規則の設定ができない点が挙げられる。

【0013】また、アクセス規則の設定を簡易に行うため、ユーザをあらかじめグループ化し、グループ単位でアクセス規則を設定する方法がある。しかし、この方法では、第4の問題として、ユーザは複数の情報システムを利用する場合にはそれぞれの情報システムごとの登録が必要になるので、ユーザの情報に変更が生じ、グルー

プ化の基準も変わった場合には、全ての情報システムにおいて、グループ情報の変更が必要になるという点が挙げられる。

【0014】そこで、ユーザ登録情報とグループ情報を少数のサーバで一括に管理し、情報システムは、ユーザ認証を行う場合やグループ情報を確認する場合には、サーバに問い合わせを行う方法が考えられる。しかし、この方法では、第5の問題として、サービスを提供する情報システムの方では、自由にユーザのグループ化を行うことができないという点が挙げられる。

【0015】本発明の目的は、アクセス主体を知らなくてもアクセス規則の設定を単純に行うことができ、しかも、アクセス主体が権限を持つことの確認も可能で、さらに、ユーザ管理の容易なアクセス制御の方法を提供することである。

【0016】

【課題を解決するための手段】本発明では、アクセス主体の一部の情報を与える、あるいは、アクセス主体の特性を記述するデータを属性と定義する。属性は、属性型と属性値から構成される。これは、JIS X 5732-1 993「開放型システム間相互接続-ディレクトリー第2部 モデル」8ページで述べられている定義である。

【0017】属性型とは、属性によって与えられる情報の項目である。例えばアクセス主体がユーザの場合、氏名(姓、名)、性別、生年月日、住所、電話番号、電子メールアドレス、組織名、会社名、部署名、役職名、免許、資格、公開鍵、などが考えられる。

【0018】属性値とは、属性型の実現値である。属性値の例としては、属性型「姓」に対して「山岡」、属性型「名」に対して「誉侍」、属性型「会社名」に対して「日本株式会社」、などである。

【0019】属性の実際の表現方法としては、「姓：山岡」、「名：誉侍」、「会社名：日本株式会社」、などと表される。

【0020】さらに、アクセス主体の属性に、その属性を証明する機関を用意する。この機関を属性CAと呼ぶことにする。属性CAは、アクセス主体の属性を証明する属性証明書の発行を行う。属性証明書は、アクセス主体の、単数あるいは複数の属性型に対する属性値が正当であることを証明するために、属性CAのデジタル署名をつけた証明書である(第3、第4の実施の形態)。

【0021】情報システムは、アクセス規則を、アクセス主体の属性、および、属性の条件式、属性の演算式、属性の論理式、などにより設定する。

【0022】アクセス主体の属性については、あるテーブルに保存し、そのテーブルを参照する方法(第1、第2の実施の形態)、あるいは、アクセス主体の側で情報システムに提示してくる方法を用いる。アクセス主体の側で情報システムに提示してくる方法としては、属性証明書(第3、第4の実施の形態)、または、公開鍵証明

書（第4の実施の形態）を用いる。

【0023】アクセス主体の実体認証にはパスワード（第1の実施の形態）、あるいは、公開鍵証明書の提示（第2～第4の実施の形態）、属性証明書の提示（第4の実施の形態）、により行う。よって、アクセス主体の登録は、情報システムやネットワークで接続されたサーバ上で一括して行う方法（第1の実施の形態）、あるいは、公開鍵CAが担当する方法（第2～第4の実施の形態）、属性CAが担当する方法（第4の実施の形態）、を用いる。

【0024】

【発明の実施の形態】図1は本発明の第1の実施の形態を示す情報システムのブロック図である。第1の実施の形態では、パスワードを用いることによりアクセス主体の実体認証を行い、テーブルに保存された属性を参照することでアクセス主体の属性を確認して、アクセス規則に基づき資源に対するアクセスを制御する。

【0025】以下、図1を参照して、第1の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【0026】まず、図1を参照して、情報システムの構成を説明する。

【0027】情報システムは、資源01を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源01の他に、アクセス要求の管理のために、実体認証手段802と、資源管理手段804と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09とを有する。

【0028】さらに、アクセス主体情報保持装置09には、識別子保持装置10と属性保持装置11とが備えられる。

【0029】また他に、パスワード情報格納装置813と属性情報テーブル814も用いるが、これらについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。外部に設ける場合、複数の情報システムに共通なサーバ上に設けることが考えられる。

【0030】以下、図1を参照して、情報システムの各構成要素の機能を説明する。

【0031】実体認証手段802は、アクセス主体の実体認証を行うための手段である。入力手段06からの識別子・パスワードの受信とそれによる起動、パスワード情報格納装置813の参照、アクセス主体の識別子・パスワードによる実体認証、識別子保持装置10への認証済アクセス主体の識別子の出力、出力手段07への認証結果の送信と起動の指令、を行う。

【0032】資源管理手段804は、資源01に対するアクセス要求の認否を判定する手段である。入力手段06からのアクセス要求の受信とそれによる起動、アクセ

ス規則テーブル08と属性保持装置11の参照、識別子保持装置10と属性情報テーブル814の参照、アクセス主体の属性の認否の判定、属性によるアクセス要求の認否の判定、属性保持装置11へのアクセス主体の是認済属性の出力、出力手段07へのアクセス不許可の送信と起動の指令、資源アクセス手段05へのアクセス要求の送信と起動の指令、を行う。

【0033】資源アクセス手段05は、資源01にアクセスできる手段である。資源管理手段804からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段07への実行結果の送信と起動の指令、を行う。

【0034】入力手段06は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力を受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【0035】出力手段07は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【0036】アクセス規則テーブル08は、資源管理手段804がアクセス権限の検査を行うために用いるテーブルであり、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。図2はアクセス規則テーブル08の設定の例である。この例では、それぞれ、日本株式会社のX部の部長にファイルAの書き込み、高等学校教諭専修免許を持つアクセス主体にデータベースBの読み出し、20才以上にサービスCの実行、の権限を与えている。この例のように、アクセス規則は、アクセス主体の属性、および、属性による条件式、属性の演算式、属性の論理式により設定することができる。

【0037】アクセス主体情報保持装置09は、アクセス主体の情報を保持する装置である。識別子保持装置10は、実体認証手段802で実体認証されたアクセス主体の識別子（例えば、登録ユーザID）を保持する装置である。属性保持装置11は、資源管理手段804で是認済のアクセス主体の属性を保持する装置である。

【0038】パスワード情報格納装置813は、実体認証手段802でアクセス主体の実体認証に用いるための識別子とパスワードに関する情報を格納する装置である。

【0039】属性情報テーブル814は、アクセス主体の識別子単位に属性を格納しているテーブルである。

【0040】以下、図1を参照して、情報システムの動作を説明する。

【0041】アクセス主体が情報システムに送信できるのは、実体認証要求とアクセス要求の二つである。

【0042】まず最初に、実体認証要求の処理を順に説明する。

【0043】アクセス主体は、識別子・パスワードを入力手段06に入力する。この入力された識別子・パスワードは入力手段06から実体認証手段802に送信されて、認証の成否の判定に用いられる。

【0044】識別子・パスワードを入力手段06から受信した実体認証手段802は、パスワード情報格納装置813からパスワード情報を読み出し、識別子・パスワードを照合し、アクセス主体の認証を行う。認証が成功した場合は、アクセス主体の識別子を識別子保持装置10に出力する。認証が失敗した場合は、識別子保持装置10へのアクセス主体の識別子の出力は行わない。また、実体認証手段802は、出力手段07に認証結果を送信して、起動を指令する。出力手段07は認証の正否の結果をアクセス主体に出力する。

【0045】次に、アクセス要求の処理を順に説明する。

【0046】アクセス要求は、アクセス主体が認証済のときに行う。アクセス主体は、資源01へのアクセス要求を入力手段06に入力する。この入力されたアクセス要求は資源管理手段804に送信される。

【0047】図3は資源管理手段804の動作の一例を示すフローチャートである。アクセス要求を入力手段06から受信した(901)資源管理手段804は、アクセス規則テーブル08を参照して、資源01のアクセスに必要な属性を抽出する(902)。例えば資源01が図2のデータベースBの場合、「免許：高等学校教諭専修」なる属性を抽出する。次に、属性保持装置11を参照してアクセスに必要な属性が是認済かを確認する(903)。属性が是認済であれば、資源01へのアクセスを認可して(904)、資源アクセス手段05にアクセス要求を送信して、起動を指令する(905)。資源アクセス手段05は、アクセス要求を資源01に対して実行し、その結果は出力手段07に送信されてアクセス主体に出力される。

【0048】属性が是認済でなければ、資源管理手段804は、識別子保持装置10を参照して、アクセス主体が認証済であるかを確認する(906)。認証済でなければ、出力手段07に認証要求の処理が必要であることを送信して、起動を指令する(907)。認証済であれば、識別子保持装置10からアクセス主体の識別子を読み出し(908)、属性情報テーブル814を参照して(909)、資源01のアクセスに必要な属性をアクセス主体が持っているかを検証する(910)。アクセス主体が該当する属性を持っていない場合は、資源01へのアクセスを不許可にして、出力手段07にアクセス不許可を送信して、起動を指令する(911)。アクセス主体が該当する属性を持っている場合は、その属性を是認して(912)、アクセス主体の属性を属性値保持装置11に出力して(913)、さらに、資源01へのアクセスを認可して(904)、資源アクセス手段05に

アクセス要求を送信して、起動を指令する(905)。

【0049】上述のように構成された本発明の第1の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者(例えばサービスの提供者)は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。

【0050】図4は本発明の第2の実施の形態を示す情報システムのブロック図である。第2の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、テーブルに保存された属性を参照することでアクセス主体の属性を確認して、アクセス規則に基づき資源に対するアクセスを制御する。

【0051】以下、図4を参照して、第2の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【0052】まず、図4を参照して、情報システムの構成を説明する。

【0053】情報システムは、資源01を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源01の他に、アクセス要求の管理のために、実体認証手段02と、資源管理手段804と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09とを有する。

【0054】さらに、アクセス主体情報保持装置09には、識別子保持装置10と属性保持装置11とが備えられる。

【0055】また他に、CA公開鍵格納装置12と属性情報テーブル814も用いるが、これらについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【0056】さらに、CA公開鍵格納装置12には、公開鍵CA公開鍵格納装置13が備えられる。

【0057】以下、図4を参照して、情報システムの各構成要素の機能を説明する。

【0058】実体認証手段02は、アクセス主体の実体認証を行うための手段である。第1の実施の形態の実体認証手段802とは異なり、認証を行うために公開鍵証明書を用いる。公開鍵証明書には、例えば図5に示すように、アクセス主体の公開鍵、アクセス主体の識別子(例えば電子メールアドレス)、氏名、証明書を発行してCAのデジタル署名が記載される。実体認証手段02は、入力手段06からの公開鍵証明書と認証情報の受信とそれによる起動、公開鍵CA公開鍵格納装置13からの公開鍵の読み出し、公開鍵証明書の公開鍵CAの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、識別子保持装置10への認証済アクセス主体の公開鍵証明書に記載の識別子の出力、出力手段07への認証結果の送信と起動の指令、を行

う。

【0059】資源管理手段804は、資源01に対するアクセス要求の認否を判定する手段である。入力手段06からのアクセス要求の受信とそれによる起動、アクセス規則テーブル08と属性保持装置11の参照、識別子保持装置10と属性情報テーブル814の参照、アクセス主体の属性の認否の判定、属性によるアクセス要求の認否の判定、属性保持装置11へのアクセス主体の是認済属性の出力、出力手段07へのアクセス不許可の送信と起動の指令、資源アクセス手段05へのアクセス要求の送信と起動の指令、を行う。

【0060】資源アクセス手段05は、資源01にアクセスできる手段である。資源管理手段804からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段07への実行結果の送信と起動の指令、を行う。

【0061】入力手段06は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力の受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【0062】出力手段07は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【0063】アクセス規則テーブル08は、資源管理手段804がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【0064】アクセス主体情報保持装置09は、アクセス主体の情報を保持する装置である。識別子保持装置10は、実体認証手段02で実体認証されたアクセス主体の、公開鍵証明書に記載されたアクセス主体の一意な識別子（例えば、電子メールアドレス）を保持する装置である。属性保持装置11は、資源管理手段804で是認済のアクセス主体の属性を保持する装置である。

【0065】属性情報テーブル814は、アクセス主体の識別子単位に属性を格納しているテーブルである。

【0066】CA公開鍵格納装置12は、第三者証明機関であるCAの公開鍵を格納しておく装置である。公開鍵CA公開鍵格納装置13は、実体認証手段02でアクセス主体の公開鍵証明書のCA署名の検証に用いるための、公開鍵CAの公開鍵を格納しておく装置である。

【0067】以下、図4を参照して、情報システムの動作を説明する。

【0068】アクセス主体が情報システムに送信できるのは、実体認証要求、アクセス要求である。

【0069】まず最初に、実体認証要求の処理を順に説明する。

【0070】アクセス主体は、公開鍵証明書を入力手段

06に入力する。この入力された公開鍵証明書は実体認証手段02に送信されて、認証の成否の判定に用いられる。

【0071】図6は実体認証手段02の動作の一例を示すフローチャートである。公開鍵証明書を入力手段06から受信した(201)実体認証手段02は、公開鍵CA公開鍵格納装置13から公開鍵CAの公開鍵を読み出し(202)、公開鍵証明書の公開鍵CAの署名の検証を行う(203)。署名の検証に失敗すれば(204)、認証は失敗で、出力手段07にCA署名無効を送信して、起動を指令する(205)。署名の検証が成功すれば(204)、公開鍵証明書からアクセス主体の公開鍵を読み出し(206)、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う(207)。認証が失敗した場合は(208)、出力手段07に送信して、起動を指令する(209)。認証が成功した場合は(208、210)、公開鍵証明書のアクセス主体の識別子(図5の場合、電子メールアドレス)を抽出して(211)、識別子保持装置10に出力する(212)。そして、出力手段07に認証成功を送信して、起動を指令する(213)。

【0072】次に、アクセス要求の処理を順に説明する。

【0073】アクセス要求は、アクセス主体が認証済のときに行う。アクセス主体は、資源01へのアクセス要求を入力手段06に入力する。この入力されたアクセス要求は資源管理手段804に送信される。第1の実施の形態と同様に、アクセス要求を入力手段06から受信した(901)資源管理手段804は、アクセス規則テーブル08を参照して、資源01のアクセスに必要な属性を抽出する(902)。さらに、属性保持装置11を参照してアクセスに必要な属性が是認済かを確認する(903)。属性が是認済であれば、資源01へのアクセスを認可して(904)、資源アクセス手段05にアクセス要求を送信して、起動を指令する(905)。資源アクセス手段05は、アクセス要求を資源01に対して実行し、その結果は出力手段07に送信されてアクセス主体に出力される。

【0074】属性が是認済でなければ、資源管理手段804は、識別子保持装置10を参照して、アクセス主体が認証済であるかを確認する(906)。認証済でなければ、出力手段07に認証要求の処理が必要であることを送信して、起動を指令する(907)。認証済であれば、識別子保持装置10からアクセス主体の識別子を読み出し(908)、属性情報テーブル814を参照して(909)、資源01のアクセスに必要な属性をアクセス主体が持っているかを検証する(910)。アクセス主体が属性を持っていない場合は、資源01へのアクセスを不許可にして、出力手段07にアクセス不許可を送

信して、起動を指令する(911)。アクセス主体が属性を持っている場合は、その属性を是認して(912)、アクセス主体の属性を属性値保持装置11に出力して(913)、さらに、資源01へのアクセスを認可して(904)、資源アクセス手段05にアクセス要求を送信して、起動を指令する(905)。

【0075】上述のように構成された本発明の第2の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者(例えばサービスの提供者)は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に公開鍵証明書を用いるので、情報システム内でのユーザ登録などの管理は必要ではなくなり、公開鍵CAの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。

【0076】図7は本発明の第3の実施の形態を示す情報システムのブロック図である。第3の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、属性証明書という新規な証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づき資源に対するアクセスを制御する。

【0077】そこでまず、属性証明書について説明する。

【0078】図8は、属性証明書を発行する属性証明書発行装置のブロック図である。属性CAは、アクセス主体の識別子・属性について、それが正当であると判断できれば、属性証明書発行装置を用いて、識別子・属性を記載した文書(属性証明書の本文)に、自身の秘密鍵でデジタル署名を行い、属性証明書を発行する。

【0079】以下、図8を用いて属性証明書発行装置の構成を説明する。

【0080】属性証明書発行装置は、識別子と属性から属性証明書の本文を作成する本文作成装置21と、属性証明書の本文にデジタル署名を行い属性証明書の署名文を作成する署名文作成装置22と、本文と署名文から属性証明書を作成する証明書作成手段23と、属性CAの秘密鍵を格納する秘密鍵格納装置601と、属性証明書の本文を保持する本文保持装置602と、属性証明書の署名文を保持する署名文保持装置603とから構成される。

【0081】以下、図8を用いて属性証明書発行装置の動作を説明する。

【0082】まず、アクセス主体の識別子・属性を、本文作成手段21に送信し、属性証明書の本文を作成して、本文保持装置602に保持する。次に、署名文作成手段22は、秘密鍵格納装置601から属性CAの秘密鍵を読み出し、秘密鍵を用いて、本文保持装置602に保持されている属性証明書の本文にデジタル署名を行

い、属性証明書の署名文を作り、署名文保持装置603に保持する。最後に、証明書作成手段23は、本文保持装置602に保持されている属性証明書の本文と、署名文保持装置603に保持されている属性証明書の署名文より、属性証明書を作成する。

【0083】図9は属性証明書の例である。701が属性証明書の本文であり、702が属性証明書の署名文である。この例では、電子メールアドレスをアクセス主体の識別子として用いている。

【0084】次に、第3の実施の形態の情報システムを、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【0085】先ず、図7を参照して、情報システムの構成を説明する。

【0086】情報システムは、資源01を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源01の他に、アクセス要求の管理のために、実体認証手段02と、属性検証手段03と、資源管理手段04と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09とを有する。

【0087】さらに、アクセス主体情報保持装置09には、識別子保持装置10と属性保持装置11とが備えられる。

【0088】また他に、CA公開鍵格納装置12も用いるが、これについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【0089】さらに、CA公開鍵格納装置12には、公開鍵CA公開鍵格納装置13と属性CA公開鍵格納装置14とが備えられる。

【0090】以下、図7を参照して、情報システムの各構成要素の機能を説明する。

【0091】実体認証手段02は、公開鍵証明書によりアクセス主体の実体認証を行うための手段である。公開鍵証明書には、例えば図5に示したように、アクセス主体の公開鍵、アクセス主体の識別子(例えば電子メールアドレス)、氏名、証明書を発行したCAのデジタル署名が記載されている。実体認証手段02は、入力手段06からの公開鍵証明書と認証情報の受信とそれによる起動、公開鍵CA公開鍵格納装置13からの公開鍵の読み出し、公開鍵証明書の公開鍵CAの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、識別子保持装置10への認証済アクセス主体の公開鍵証明書に記載の識別子の出力、出力手段07への認証結果の送信と起動の指令、を行う。

【0092】属性検証手段03は、属性証明書を用いてアクセス主体の属性の認否の判定を行うための手段である。属性証明書には、例えば図9に示したように、アクセス主体の属性、アクセス主体の識別子(公開証明書と

同じもので、例えば電子メールアドレス)、証明書を発行したCAのデジタル署名が記載されている。属性検証手段03は、入力手段06からの属性証明書の受信とそれによる起動、識別子保持装置10の参照、属性CA公開鍵格納装置14からの公開鍵の読み出し、属性証明書の属性CAの署名の検証、アクセス主体の属性の認否の判定、および、属性保持装置11へのアクセス主体の是認属性の出力、出力手段07への属性検証結果の送信と起動の指令、を行う。

【0093】資源管理手段04は、資源01に対するアクセス要求の認否を判定する手段である。入力手段06からのアクセス要求の受信とそれによる起動、アクセス規則テーブル08と属性保持装置11の参照、属性によるアクセス要求の認否の判定、出力手段07へのアクセス不許可の送信と起動の指令、資源アクセス手段05へのアクセス要求の送信と起動の指令、を行う。

【0094】資源アクセス手段05は、資源01にアクセスできる手段である。資源管理手段04からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段07への実行結果の送信と起動の指令、を行う。

【0095】入力手段06は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力を受信、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【0096】出力手段07は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【0097】アクセス規則テーブル08は、資源管理手段04がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【0098】アクセス主体情報保持装置09は、アクセス主体の情報を保持する装置である。識別子保持装置10は、実体認証手段02で実体認証されたアクセス主体の、公開鍵証明書に記載されたアクセス主体の一意な識別子(例えば、電子メールアドレス)を保持する装置である。属性保持装置11は、属性検証手段03で是認済のアクセス主体の属性を保持する装置である。

【0099】CA公開鍵格納装置12は、第三者証明機関であるCAの公開鍵を格納しておく装置である。公開鍵CA公開鍵格納装置13は、実体認証手段02でアクセス主体の公開鍵証明書のCA署名の検証に用いるための、公開鍵CAの公開鍵を格納しておく装置である。属性CA公開鍵格納装置14は、属性検証手段03でアクセス主体の属性証明書のCA署名の検証に用いるための、属性CAの公開鍵を格納しておく装置である。

【0100】以下、図7を参照して、情報システムの動

作を説明する。

【0101】アクセス主体は情報システムに、実体認証要求、属性是認要求、アクセス要求を送信できる。

【0102】まず最初に、実体認証要求の処理を順に説明する。

【0103】アクセス主体は、公開鍵証明書を入力手段06に入力する。この入力された公開鍵証明書は実体認証手段02に送信されて、認証の成否の判定に用いられる。公開鍵証明書を入力手段06から受信した実体認証手段02は、第2の実施の形態と同様に、公開鍵CA公開鍵格納装置13から公開鍵CAの公開鍵を読み出し(202)、公開鍵証明書の公開鍵CAの署名の検証を行う(203)。署名の検証に失敗すれば(204)、認証は失敗で、出力手段07にCA署名無効を送信して、起動を指令する(205)。署名の検証が成功すれば(204)、公開鍵証明書からアクセス主体の公開鍵を読み出し(206)、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う(207)。認証が失敗した場合は(208)、出力手段07に送信して、起動を指令する(209)。認証が成功した場合は(208、210)、公開鍵証明書のアクセス主体の識別子(図5の場合、電子メールアドレス)を抽出して(211)、識別子保持装置10に出力する(212)。そして、出力手段07に認証成功を送信して、起動を指令する(213)。

【0104】次に、属性是認要求の処理を順に説明する。

【0105】属性是認要求は、アクセス主体が認証済のときに行う。アクセス主体は、入力手段06に属性証明書をを入力する。この入力された属性証明書は属性検証手段03に送信されて、属性の認否の検証に用いられる。

【0106】図10は属性検証手段03の動作の一例を示すフローチャートである。属性証明書を入力手段06から受信した(301)属性検証手段03は、属性証明書からアクセス主体の識別子を抽出する(302)。次に、識別子保持装置10を参照して、アクセス主体が認証済であるかを確認する(303)。認証済でなければ、出力手段07に認証要求の処理が必要であることを送信して、起動を指令する(304)。認証済であれば、識別子保持装置10からアクセス主体の識別子を読み出し(305)、属性証明書のアクセス主体の識別子と一致するかを確認する(306)。一致しなければ、出力手段07に識別子の不一致を送信して、起動を指令する(307)。一致すれば、属性証明書はアクセス主体のものであると判断でき、属性CA公開鍵格納装置14から属性CAの公開鍵を読み出し(308)、属性証明書の属性CAの署名の検証を行う(309)。署名の検証に失敗すれば(310)、出力手段07にCA署名無効を送信して、起動を指令する(311)。署名の検

証に成功すれば(310)、属性は是認されて(312)、属性を属性保持装置11に出力する(313)。そして、出力手段07に属性是認を送信して、起動を指令する(314)。

【0107】次に、アクセス要求の処理を順に説明する。アクセス要求は、アクセス主体が属性是認済のときに行う。アクセス主体は、資源01へのアクセス要求を入力手段06に入力する。この入力されたアクセス要求は資源管理手段04に送信される。

【0108】図11は資源管理手段04の動作の一例を示すフローチャートである。アクセス要求を入力手段06から受信した(401)資源管理手段04は、アクセス規則テーブル08を参照して、資源01のアクセスに必要な属性を抽出する(402)。さらに、属性保持装置11を参照してアクセスに必要な属性が是認済を確認する(403)。属性が是認済であれば、資源01へのアクセスを認可して(404)、資源アクセス手段05にアクセス要求を送信して、起動を指令する(405)。資源アクセス手段05は、アクセス要求を資源01に対して実行し、その結果は出力手段07に送信されてアクセス主体に出力される。属性が是認済でなければ、出力手段07に属性是認要求の処理が必要であることを送信して、起動を指令する(406)。

【0109】上述のように構成された本発明の第3の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者(例えばサービスの提供者)は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に公開鍵証明書を用いるので、情報システム内でのユーザ登録などの管理は必要でなくなり、公開鍵CAの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要でなくなる。またさらに、属性証明書を用いるので、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性是認も容易に行える。さらにそれぞれの属性CAがアクセス主体の一部の情報の属性のみを管理すればよいので複雑な作業にはならない。

【0110】図12は本発明の第4の実施の形態を示す情報システムのブロック図である。第4の実施の形態では、公開鍵証明書を用いることによりアクセス主体の実体認証を行い、且つ、その公開鍵証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づいて資源に対するアクセスを制御する。また、属性証明書の属性にアクセス主体の公開鍵が記載されている場合は、属性証明書を用いることによりアクセス主体の実体認証を行い、且つ、その属性証明書に記載されたアクセス主体の属性を是認して、アクセス規則に基づいて資源に対するアクセスを制御することもできる。即ち、第4の実

施の形態では、1つの証明書で実体認証と属性の是認とを行う。

【0111】第4の実施の形態では、図5に示した公開鍵証明書の内容に、更に、アクセス主体の属性を追加した、例えば図13に例示するような公開鍵証明書を用いることができる。

【0112】また、第4の実施の形態では、図9に示した属性証明書の内容に、更に、アクセス主体の公開鍵を追加した、例えば図14に例示するような属性証明書を用いることができる。なお、属性証明書の本文701に記載される識別子には、アクセス主体の公開鍵を用いることも出来る。この場合、匿名性のある属性証明書を作成することが出来る。このような属性証明書は、図8に示した属性証明書発行装置において、入力した識別子としてアクセス主体の公開鍵を与えることで作成することができる。

【0113】以下、図12を参照して、第4の実施の形態を、情報システムの構成、各構成要素の機能、情報システムの動作の順で説明する。

【0114】まず、情報システムの構成を説明する。

【0115】情報システムは、資源01を備え、アクセス主体からのアクセス要求などを管理する。また、情報システムは、資源01の他に、アクセス要求の管理のために、属性検証手段1103と、資源管理手段04と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09とを有する。

【0116】さらに、アクセス主体情報保持装置09には、属性保持装置11が備えられる。

【0117】また他に、CA公開鍵格納装置12も用いるが、これについては情報システム内の装置として構成してもよいし、ネットワークで接続された外部に存在してもよい。

【0118】さらに、CA公開鍵格納装置12には、公開鍵CA公開鍵格納装置13と属性CA公開鍵格納装置14とが備えられる。

【0119】以下、図12を参照して、情報システムの各構成要素の機能を説明する。

【0120】属性検証手段1103は、公開鍵証明書または属性証明書を用いてアクセス主体の実体認証と属性検証とを行うための手段である。入力手段06からの公開鍵証明書と認証情報の受信とそれによる起動、入力手段06からの属性証明書と認証情報の受信とそれによる起動、公開鍵CA公開鍵格納装置13からの公開鍵の読み出し、属性CA公開鍵格納装置14からの公開鍵の読み出し、公開鍵証明書の公開鍵CAの署名の検証、属性証明書の属性CAの署名の検証、アクセス主体の非対称暗号系における認証方法による実体認証、および、属性保持装置11へのアクセス主体の是認済属性の出力、出力手段07への認証結果の送信と起動の指令、を行う。

【0121】資源管理手段04は、資源01に対するアクセス要求の認否を判定する手段である。入力手段06からのアクセス要求の受信とそれによる起動、アクセス規則テーブル08と属性保持装置11の参照、属性によるアクセス要求の認否の判定、出力手段07へのアクセス不許可の送信と起動の指令、資源アクセス手段05へのアクセス要求の送信と起動の指令、を行う。

【0122】資源アクセス手段05は、資源01にアクセスできる手段である。資源管理手段04からのアクセス要求の受信とそれによる起動、アクセス要求の実行、出力手段07への実行結果の送信と起動の指令、を行う。

【0123】入力手段06は、アクセス主体と情報システムとの対話を行う手段である。アクセス主体からのアクセス要求などの入力、情報システム内の他の手段への情報の送信と起動の指令、を行う。

【0124】出力手段07は、アクセス主体と情報システムとの対話を行う手段である。情報システム内の他の手段からの情報の受信とそれによる起動、アクセス主体に対する処理結果などの出力、を行う。

【0125】アクセス規則テーブル08は、資源管理手段04がアクセス権限の検査を行うために用いるテーブルであり、例えば図2に示したように、情報システム内の全ての資源に対して、その資源にアクセス可能な属性が設定してある。

【0126】アクセス主体情報保持装置09は、アクセス主体の情報を保持する装置である。属性保持装置11は、属性検証手段1103で是認済のアクセス主体の属性を保持する装置である。第3の実施の形態と異なり、識別子保持装置10は必要ない。

【0127】CA公開鍵格納装置12は、第三者証明機関であるCAの公開鍵を格納しておく装置である。公開鍵CA公開鍵格納装置13は、属性検証手段1103でアクセス主体の公開鍵証明書のCA署名の検証に用いるための、公開鍵CAの公開鍵を格納しておく装置である。属性CA公開鍵格納装置14は、属性検証手段1103でアクセス主体の属性証明書のCA署名の検証に用いるための、属性CAの公開鍵を格納しておく装置である。

【0128】以下、図12を参照して、情報システムの動作を説明する。

【0129】第4の実施の形態では、実体認証要求は送信しない。属性是認要求のときに、実体認証を行う。従って、アクセス主体は情報システムに、属性是認要求、アクセスが送信できる。

【0130】まず、属性是認要求の処理を順に説明する。

【0131】アクセス主体は、入力手段06に公開鍵証明書または属性証明書をを入力する。入力された公開鍵証明書または属性証明書は、属性検証手段1103に送信

されて、認証の成否の判定に用いられ、属性の認否の検証がされる。

【0132】図15は属性検証手段1103の動作の一例を示すフローチャートである。属性証明書をを入力手段06から受信した(1201)属性検証手段1103は、属性CA公開鍵格納装置14から属性CAの公開鍵を読み出し(1202)、属性証明書の属性CAの署名の検証を行う(1203)。署名の検証に失敗すれば(1204)、出力手段07にCA署名無効を送信して、起動を指令する(1205)。署名の検証が成功すれば(1204)、属性証明書からアクセス主体の公開鍵を読み出し(1206)、アクセス主体の秘密鍵で正当性を主張する非対称暗号系における認証方法により、アクセス主体の実体認証を行う(1207)。認証が失敗した場合は(1208)、出力手段07に送信して、起動を指令する(1209)。認証が成功した場合は(1208、1210)、属性証明書のアクセス主体の属性を抽出して(1211)、属性保持装置11に出力する(1212)。そして、出力手段07に属性是認を送信して、起動を指令する(1213)。また、1201で属性証明書でなく、公開鍵証明書を受信した場合も、属性CA公開鍵格納装置14の代わりに、公開鍵CA公開鍵格納装置13から公開鍵CAの公開鍵を読み出すが、その他についての処理は同様である。

【0133】次に、アクセス要求の処理を順に説明する。アクセス要求は、アクセス主体が属性是認済のときに行う。アクセス主体は、資源01へのアクセス要求を入力手段06に入力する。この入力されたアクセス要求は資源管理手段04に送信される。アクセス要求を入力手段06から受信した資源管理手段04は、第3の実施の形態と同様に、アクセス規則テーブル08を参照して、資源01のアクセスに必要な属性を抽出する(402)。さらに、属性保持装置11を参照してアクセスに必要な属性が是認済かを確認する(403)。属性が是認済であれば、資源01へのアクセスを認可して(404)、資源アクセス手段05にアクセス要求を送信して、起動を指令する(405)。資源アクセス手段05は、アクセス要求を資源01に対して実行し、その結果は出力手段07に送信されてアクセス主体に出力される。属性が是認済でなければ、出力手段07に属性是認要求の処理が必要であることを送信して、起動を指令する(406)。

【0134】上述のように構成された本発明の第4の実施の形態によれば、アクセス主体の属性によりアクセス規則の設定を行うため、アクセス規則の設定が単純に行える。それにより、資源のアクセス規則の設定者(例えばサービスの提供者)は、アクセス主体を知らない場合でもアクセスを許可することが可能となる。また、アクセス主体の実体認証に属性証明書または公開鍵証明書をを用いるので、情報システム内でのユーザ登録などの管理

は必要ではなくなり、公開鍵CAの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。またさらに、属性証明書または公開鍵証明書によって、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性は認も容易に行える。さらにそれぞれの属性CAがアクセス主体の一部の情報の属性のみを管理すればよいので複雑な作業にはならない。また、1つの証明書でアクセス主体の実体認証と属性の是認とを行うことができる。

【0135】図16は本発明を適用した情報システムのハードウェア構成例を示すブロック図である。この情報システムは、CPUやメモリ等を有するコンピュータ1601と、アクセス主体となるユーザが利用する利用者端末1602と、記録媒体1603とから構成される。記録媒体1603は、CD-ROM、磁気ディスク装置、半導体メモリ等の機械読み取り可能な記録媒体であり、ここに記録されたアクセス制御用プログラムは、コンピュータ1601に読み取られ、コンピュータ1601の動作を制御し、コンピュータ1601上に前述した

第1、第2、第3または第4の実施の形態における各構成要素を実現する。

【0136】即ち、第1の実施の形態にあっては、コンピュータ1601上に、実体認証手段802と、資源管理手段804と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09と、必要に応じてパスワード情報格納装置813および属性情報テーブル814とを実現する。

【0137】また、第2の実施の形態にあっては、コンピュータ1601上に、実体認証手段02と、資源管理手段804と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09と、必要に応じてCA公開鍵格納装置12および属性情報テーブル814とを実現する。

【0138】さらに、第3の実施の形態にあっては、コンピュータ1601上に、実体認証手段02と、属性検証手段03と、資源管理手段04と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09と、必要に応じてCA公開鍵格納装置12とを実現する。

【0139】また更に、第4の実施の形態にあっては、コンピュータ1601上に、属性検証手段1103と、資源管理手段04と、資源アクセス手段05と、入力手段06と、出力手段07と、アクセス規則テーブル08と、アクセス主体情報保持装置09と、必要に応じてCA公開鍵格納装置12とを実現する。

【0140】

【発明の効果】本発明の効果としては、アクセス規則の

設定が単純に行えることが挙げられる。これは、アクセス主体の属性により、アクセス規則の設定を行うためである。それにより、資源のアクセス規則の設定者（例えばサービスの提供者）は、アクセス主体を知らない場合でもアクセスを許可することができる。

【0141】また、アクセス主体の実体認証に公開鍵証明書を利用すれば、情報システム内でのユーザ登録などの管理は必要ではなくなり、公開鍵CAの公開鍵の保管のみを行えばよい。さらに、ユーザ情報はアクセス主体の方で提示してくるので、ユーザ登録の検索などの処理も必要ではなくなる。

【0142】さらに、属性証明書をいれれば、多種多様の属性をアクセス主体の方で提示することができて、情報システムでの属性は認も容易に行える。さらにそれぞれの属性CAがアクセス主体の一部の情報の属性のみを管理すればよいので複雑な作業にはならない。

【0143】これにより、情報システムでは限定された登録ユーザのみではなく、不特定多数のアクセス主体にサービスを提供することが可能になる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における情報システムの構成を示すブロック図である。

【図2】本発明の第1～第4の実施の形態におけるアクセス規則テーブル08の例を示す図である。

【図3】本発明の第1、第2の実施の形態における資源管理手段804の動作を示すフローチャートである。

【図4】本発明の第2の実施の形態における情報システムの構成を示すブロック図である。

【図5】公開鍵証明書の例を示す図である。

【図6】本発明の第2、第3の実施の形態における実体認証手段02の動作を示すフローチャートである。

【図7】本発明の第3の実施の形態における情報システムの構成を示すブロック図である。

【図8】本発明の第3、第4の実施の形態における属性証明書発行装置の構成を示すブロック図である。

【図9】本発明の第3の実施の形態における属性証明書の例を示す図である。

【図10】本発明の第3の実施の形態における属性検証手段03の動作を示すフローチャートである。

【図11】本発明の第3、第4の実施の形態における資源管理手段04の動作を示すフローチャートである。

【図12】本発明の第4の実施の形態における情報システムの構成を示すブロック図である。

【図13】アクセス主体の属性の記述を含む公開鍵証明書の例を示す図である。

【図14】本発明の第4の実施の形態における属性証明書の例を示す図である。

【図15】本発明の第4の実施の形態における属性検証手段1103の動作を示すフローチャートである。

【図16】本発明を適用した情報システムのハードウェア

ア構成例を示すブロック図である。

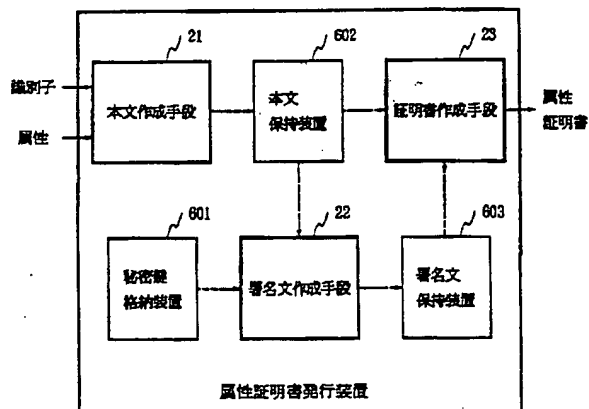
【符号の説明】

- 01 資源
- 02 実体認証手段
- 03 属性検証手段
- 04 資源管理手段
- 05 資源アクセス手段
- 06 入力手段
- 07 出力手段
- 08 アクセス規則テーブル
- 09 アクセス主体情報保持装置
- 10 識別子保持装置

【図2】

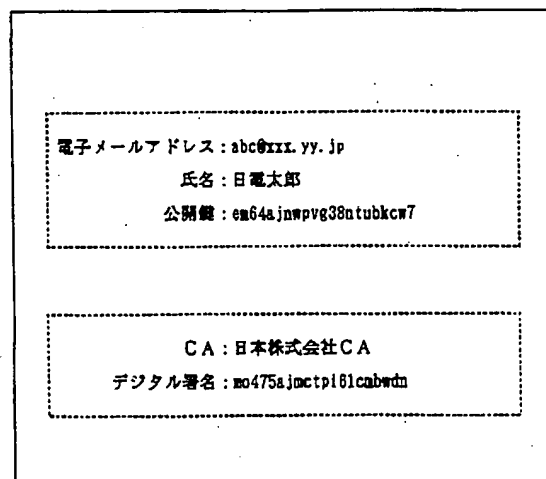
属性 \ 資源	ファイルA	データベースB	サービスC
会社名: 日本株式会社 部署名: X部 役職名: 部長	書き込み可能		
免許: 高等学校教諭専修		読み出し可能	
現在年月日-生年月日>-20年			実行可能

【図8】

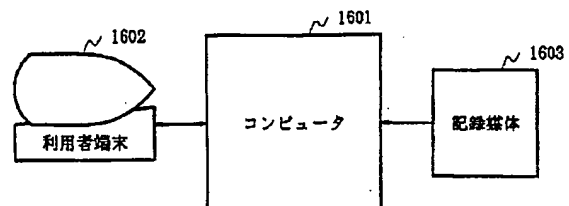


- * 11 属性保持装置
- 12 CA公開鍵格納装置
- 13 公開鍵CA公開鍵格納装置
- 14 属性CA公開鍵格納装置
- 21 本文作成手段
- 22 署名文作成手段
- 23 証明書作成手段
- 802 実体認証手段
- 804 資源管理手段
- 10 813 パスワード情報格納装置
- 814 属性情報テーブル
- * 1103 属性検証手段

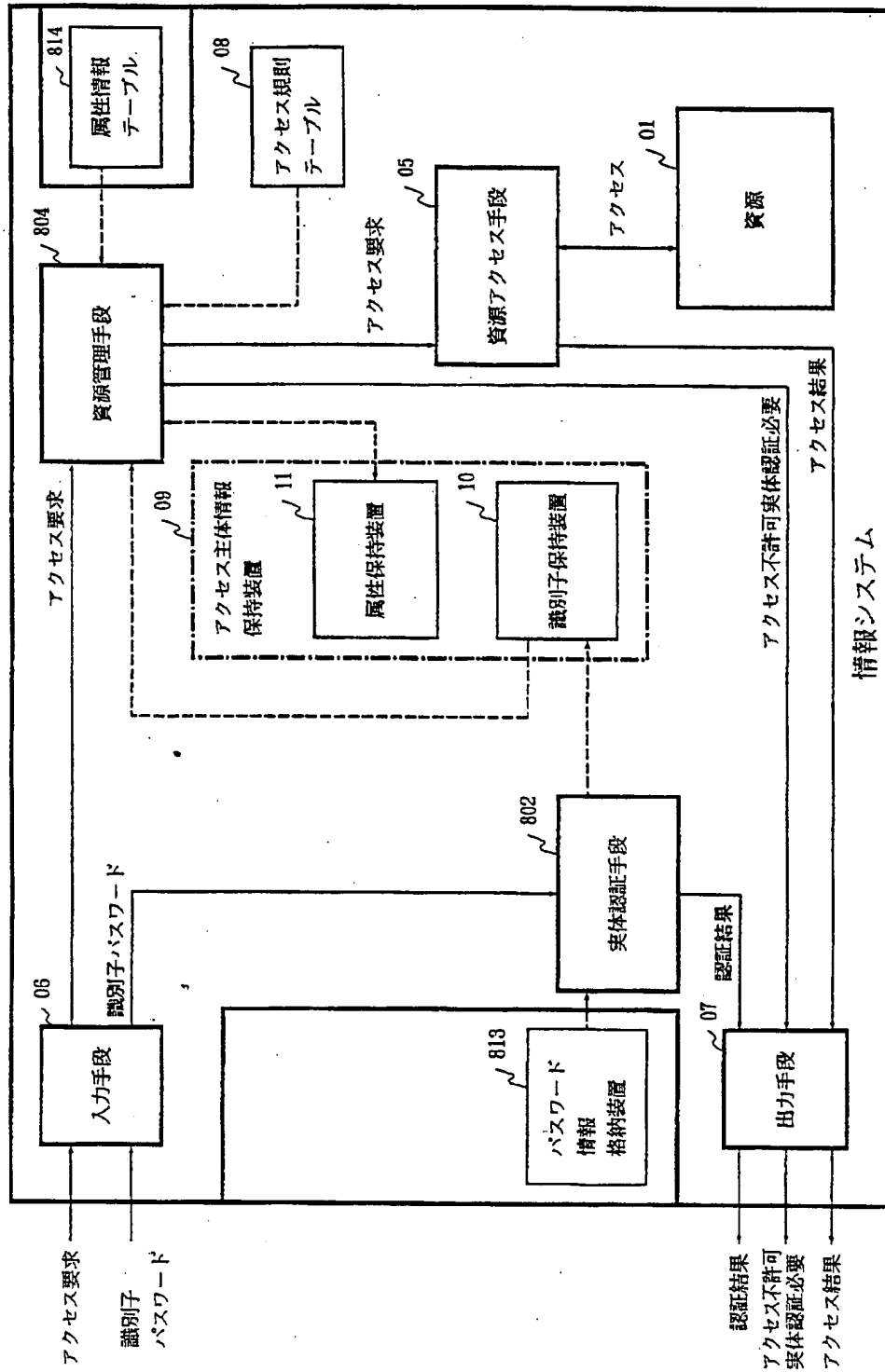
【図5】



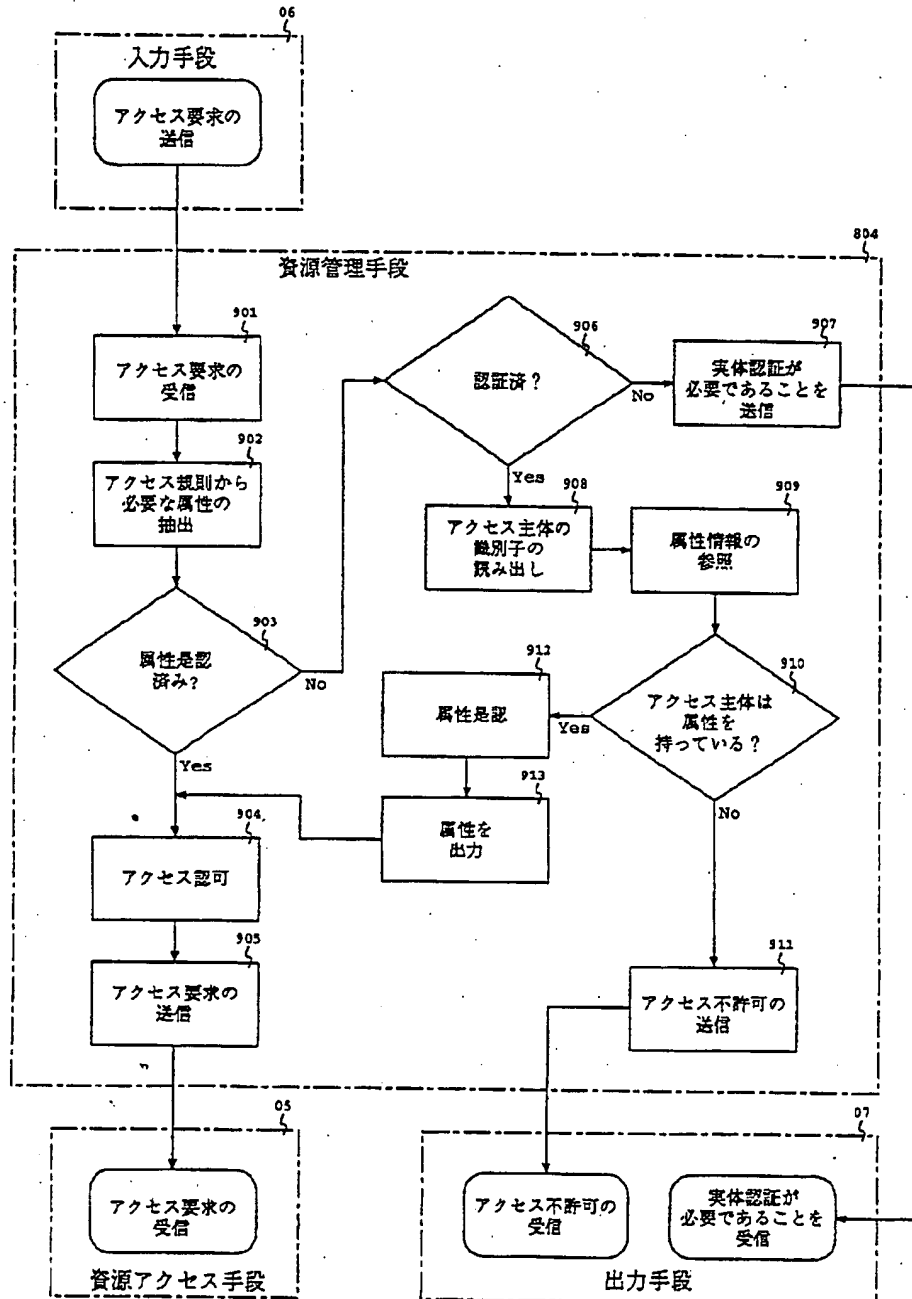
【図16】



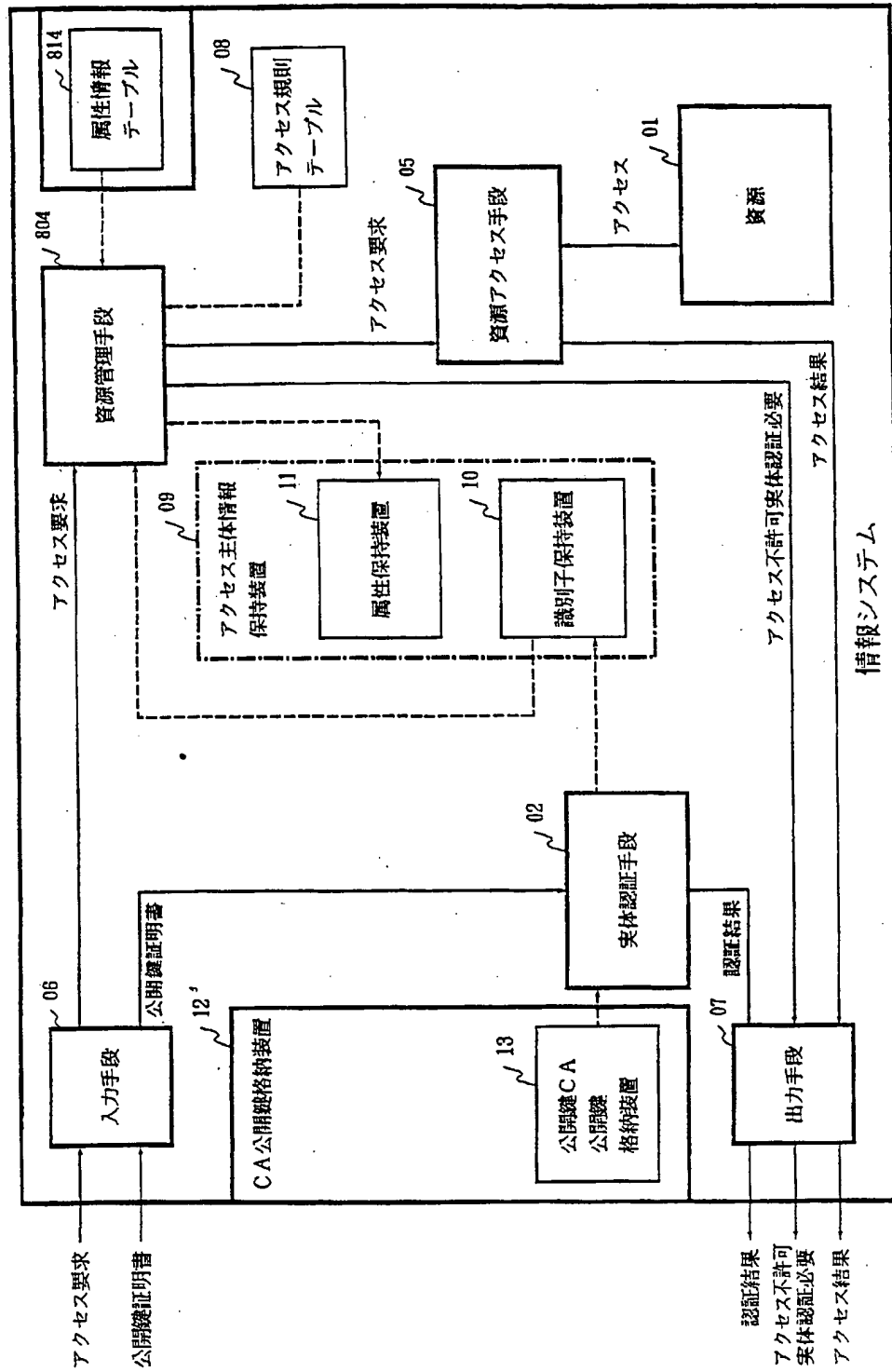
【図1】



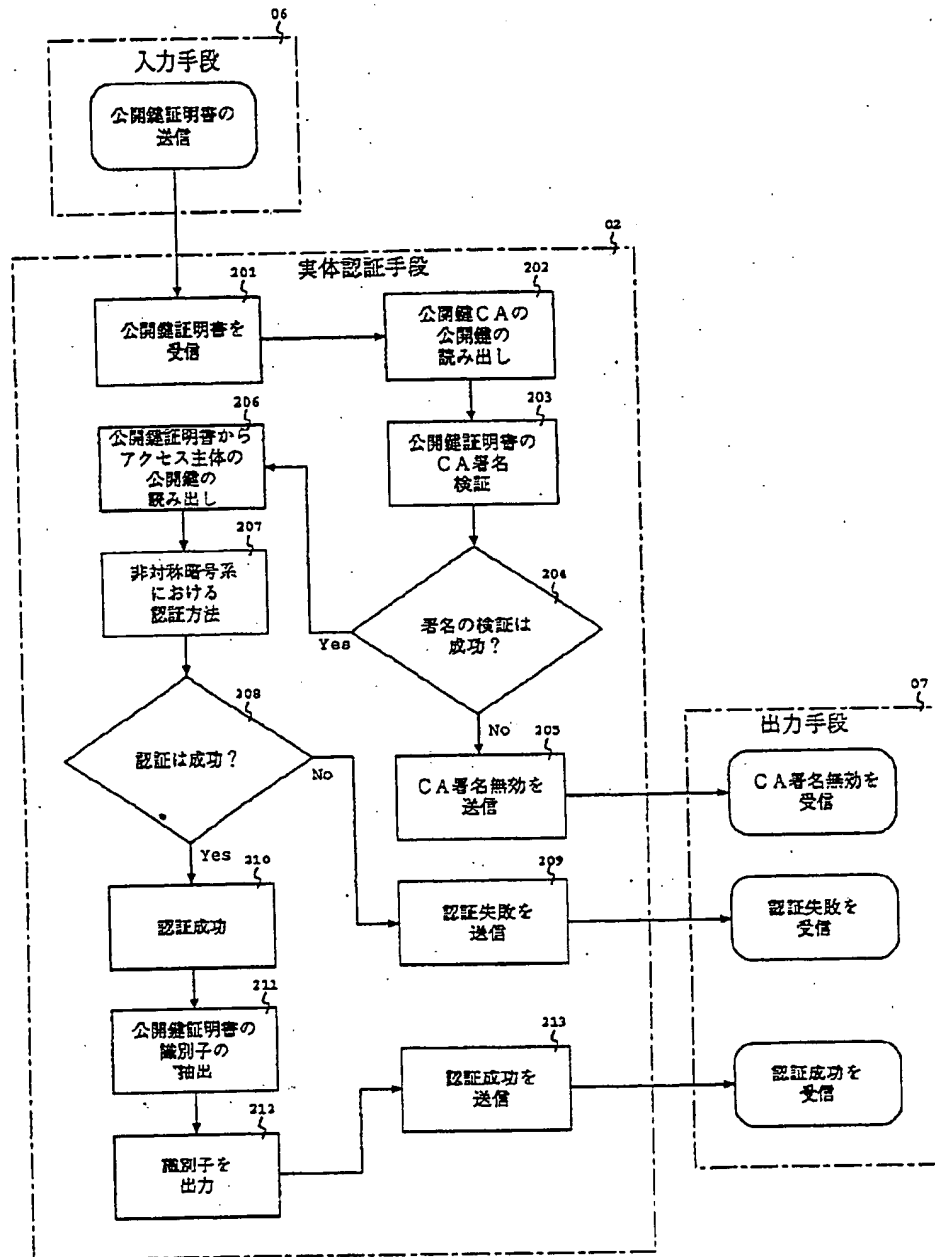
【図3】



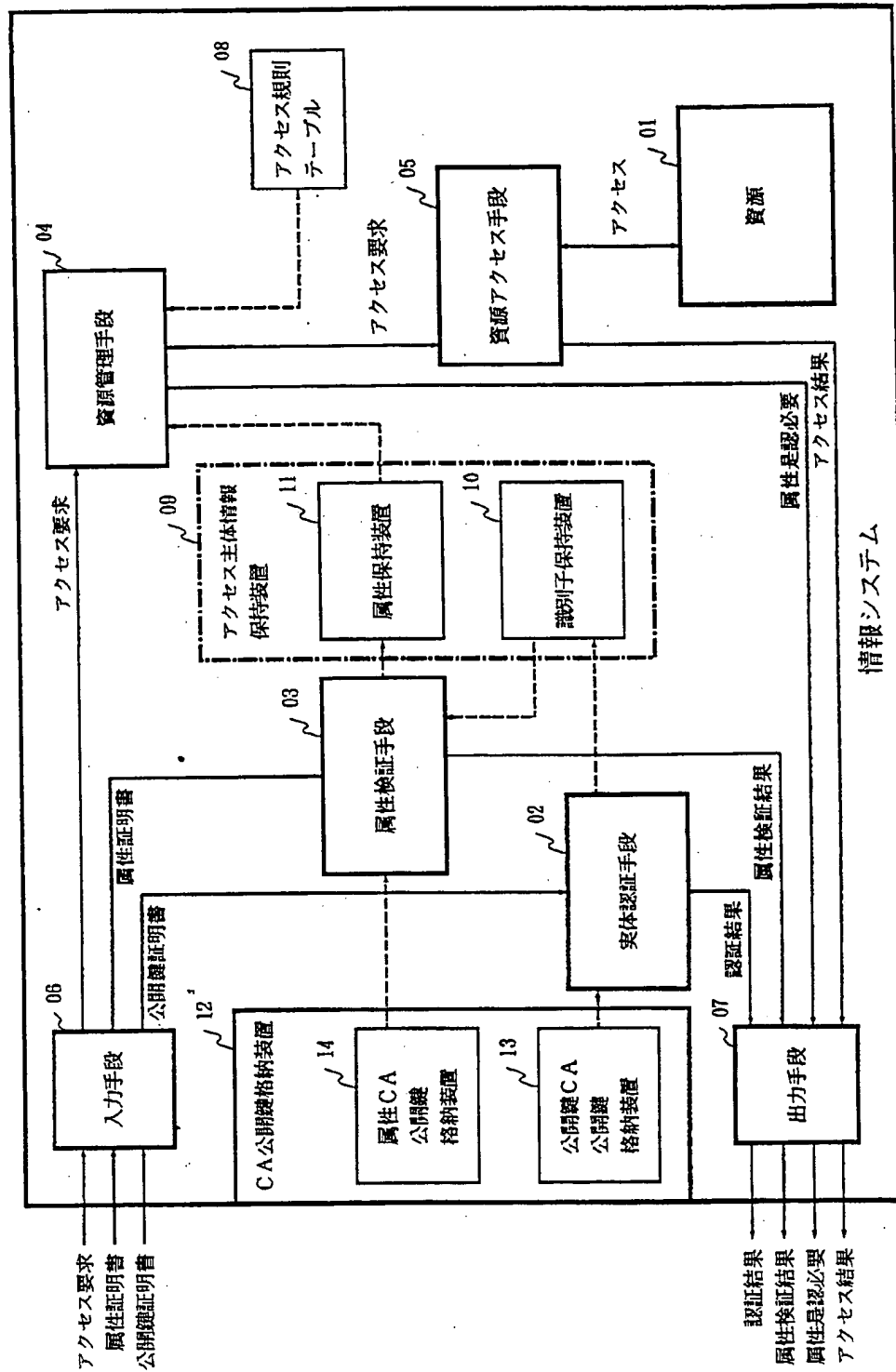
【図4】



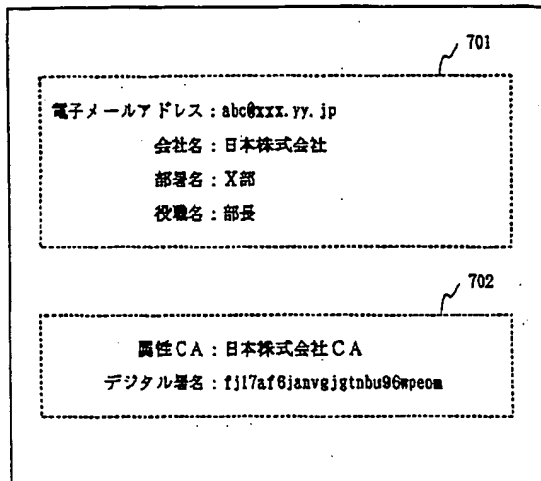
【図6】



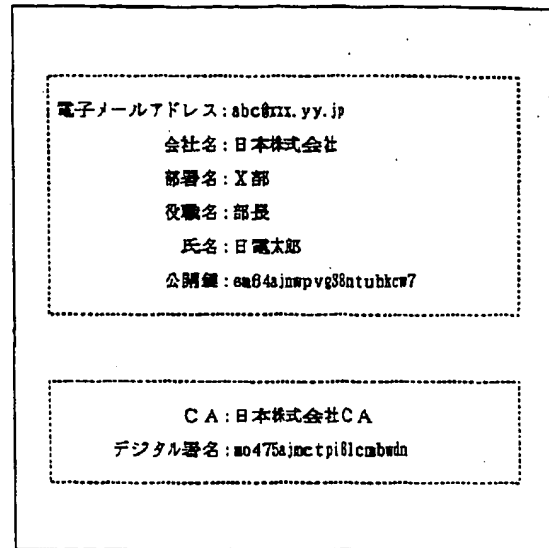
【図7】



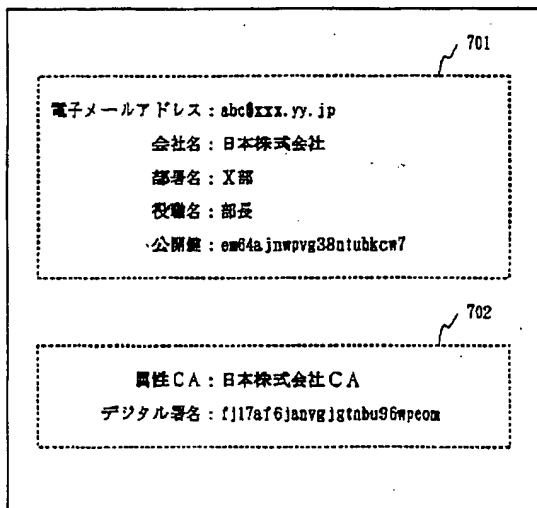
【図9】



【図13】



【図14】



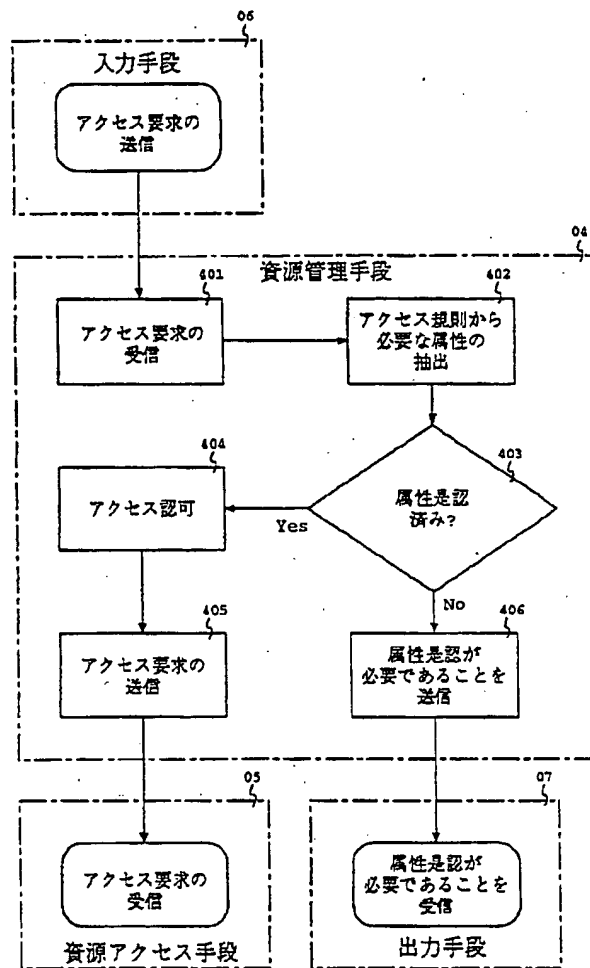
The flowchart illustrates the attribute verification process, starting with an input method (入力手段) and an attribute verification method (属性検証手段). The process involves receiving an attribute certificate (属性証明書), extracting its identifier (識別子), and checking if it is a valid certificate (認証済?). If not, it checks for real authentication (実体認証) and sends the identifier inconsistency (識別子の不一致) to the output method (出力手段). If it is a valid certificate, it checks if the identifier is consistent (識別子は一致?). If not, it checks for real authentication and sends the identifier inconsistency. If consistent, it checks the CA's public key (属性CAの公開鍵), then the attribute certificate's CA signature (属性証明書のCA署名検証). If the signature verification fails (署名の検証は成功?), it sends the CA signature invalidity (CA署名無効) to the output method. If successful, it outputs the attribute (属性を出力) and sends the attribute recognition (属性是認) to the output method.

```

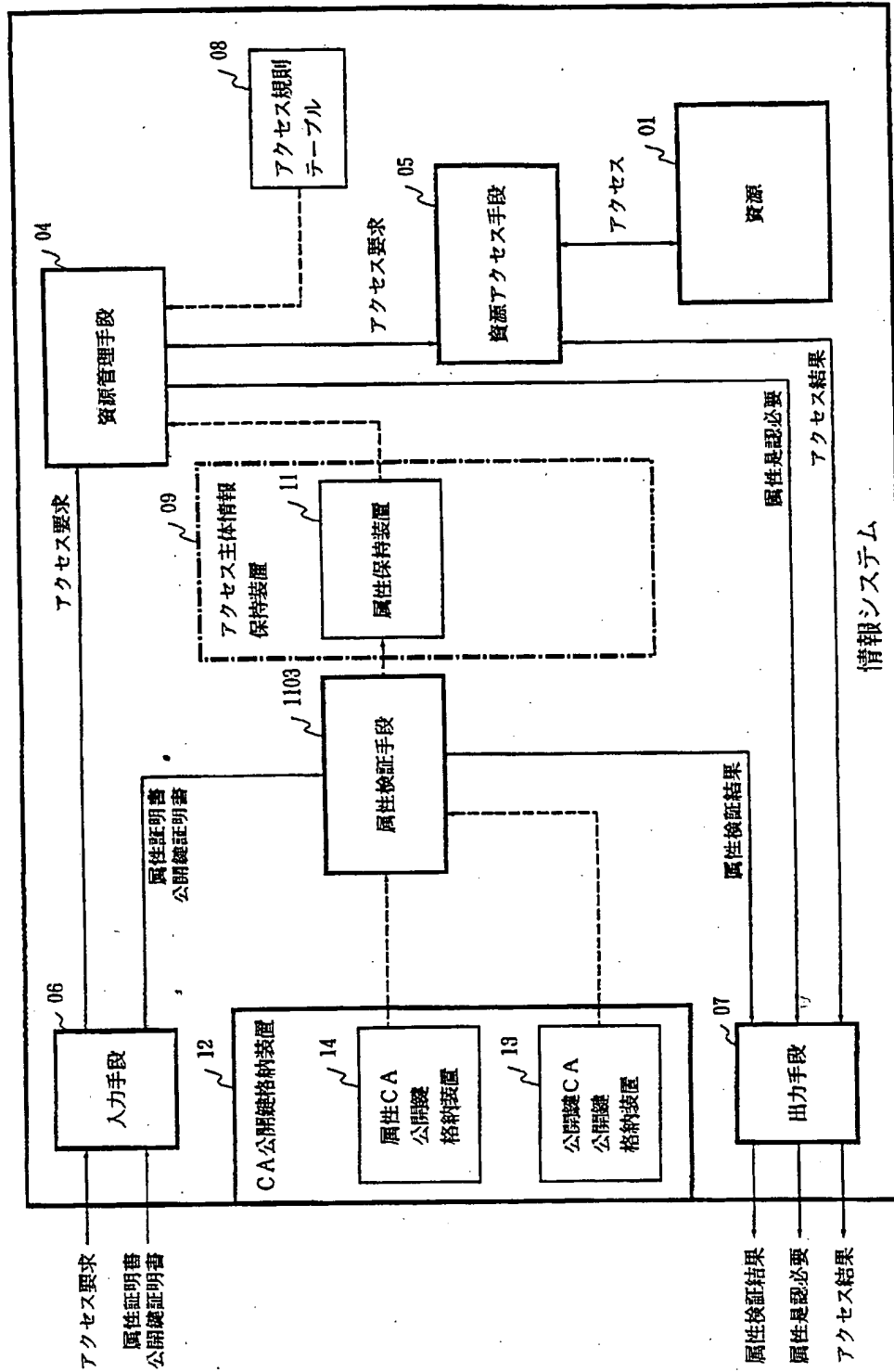
graph TD
    subgraph InputMethod [入力手段]
        A[属性証明書の送信]
    end
    subgraph AttributeVerificationMethod [属性検証手段]
        B[属性証明書の受信] --> C[属性証明書の識別子の抽出]
        C --> D{認証済?}
        D -- Yes --> E[アクセス主体の識別子の読み出し]
        E --> F{識別子は一致?}
        F -- No --> G[実体認証が必要であることを送信]
        F -- Yes --> H[属性CAの公開鍵の読み出し]
        H --> I[属性証明書のCA署名検証]
        I --> J{署名の検証は成功?}
        J -- No --> K[CA署名無効を送信]
        J -- Yes --> L[属性を出力]
        L --> M[属性是認を送信]
    end
    subgraph OutputMethod [出力手段]
        N[実体認証が必要であることを受信]
        O[識別子の不一致を受信]
        P[CA署名無効を受信]
        Q[属性是認を受信]
    end
    G --> N
    M --> Q
    D -- No --> O
    K --> P

```

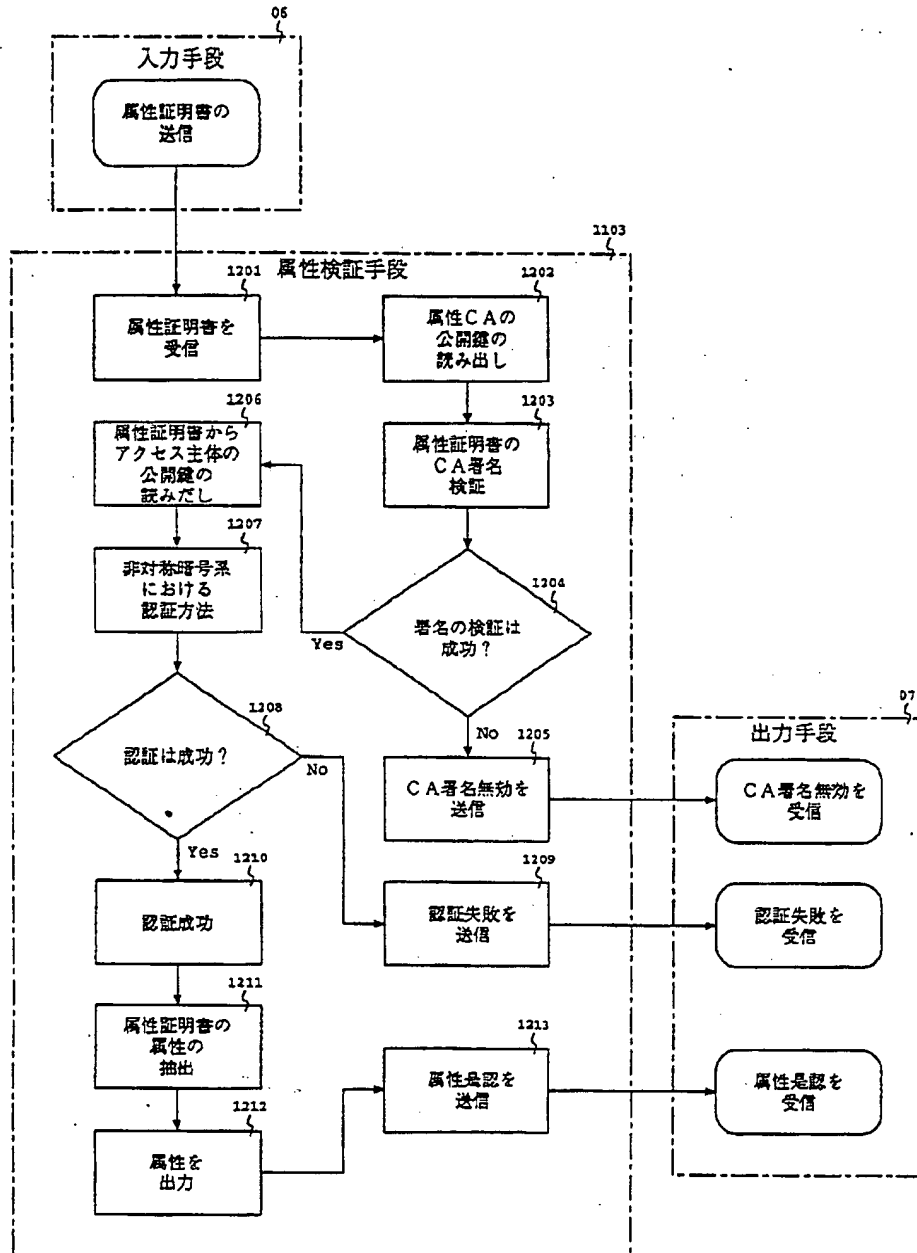
【図11】



【図12】



【図15】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.